REMARKS/ARGUMENTS

Favorable reconsideration of this application is respectfully requested.

Claim 1 is amended by the present response to address the informality therein by now referring to "device information".

Claims 1-3 and 5-17 are pending in this application. Claim 4 is canceled by the present response without prejudice. Claims 5-8 and 11-17 stand withdrawn from consideration as directed to a non-elected invention. Claims 1-2 and 9-10 were rejected under 35 U.S.C. § 102(e) as anticipated by U.S. patent 6,185,680 to Shimbo et al. (herein "Shimbo"). Claims 3 and 4 were rejected under 35 U.S.C. § 103(a) as unpatentable over Shimbo in view of U.S. patent 6,735,313 to Bleichenbacher et al. (herein "Bleichenbacher").

Addressing the above-noted prior art rejections, those rejections are traversed by the response.

Initially, applicants note independent claim 1 is amended by the present response to clarify features recited therein. Specifically, independent claim 1 now clarifies that the device ID "is formed of numerals each indicating a position of a device key in each one dimensional array of the device key matrix and indicates a path in a plurality of trees that are formed of all possible combinations of device keys in the device key matrix". That claimed subject matter is believed to be fully supported by the original specification, for example at page 27, line 17 to page 39, line 20, and see particularly page 27, line 17 to page 28, line 13. Independent claim 9 is similarly amended.

The outstanding rejection cites Shimbo to disclose device keys arranged in a two-dimensional manner at column 21, lines 1-10 and Figure 6, and to disclose a device key selecting unit at column 21, lines 35-43. However, Shimbo is not believed to disclose the features now recited in the claims.

The present invention is directed to a system that (i) assigns a device ID and a plurality of device keys corresponding to the device ID, with respect to each of a plurality of content utilizing devices, which decrypt encrypted contents distributed thereto; (ii) encrypts a master key (which is required for decrypting the encrypted contents), so that it enables the device keys (assigned to each content utilizing device) to decrypt the encrypted contents; and (iii) distributes the master key to the content utilizing device. The present invention can be particularly directed to a technique of inhibiting a content utilizing device targeted for revoke from decrypting a master key.

As discussed in the present specification at page 27, line 17 to page 28, line 13 each numeral of the device ID indicates a position of a device key in each one dimensional array of the device key matrix. Further, the device ID indicates a path in the plurality of trees that are formed of all possible combinations of device keys in the device key matrix.

A master key is encrypted to enable decryption using path function values calculated from a combination of device keys on a partial path, which is included in the path indicated by a device ID of a device other than the content utilizing device targeted for revoke. The master key is distributed after being encrypted.

The content utilizing device uses the path function values, which have been calculated based on the device keys on a partial path included in the path indicated by the device ID, to decrypt the master key.

To inhibit the content utilizing device targeted for revoke from decrypting a master key (i.e., to inhibit the device from decrypting the content using the device key on the partial path included in the path indicated by the device ID of the content utilizing device targeted for revoke), a master key is encrypted using path function values calculated from a combination of device keys on a path that does not include a partial path, which is included in the path indicated by the device ID of the content utilizing device targeted for revoke.

Thereby, the claimed invention can operate in a method of assigning the above-described device ID and a device key corresponding to the device ID, to enable the above-described revoke control.

Shimbo is directed to a packet authentication packet encryption/decryption scheme for a security gateway. In the cited passages in Shimbo at column 21, lines 1-10 and 35-53 Shimbo discloses an authentication key management unit 503 that manages an authentication table to store authentication keys, and an authentication key management unit 803 managing an authentication table. Shimbo further discloses an authentication code inspection unit 604 that inspects a properness of the authentication code.

However, Shimbo does not disclose or suggest (i) each numeral of the device ID indicates a position of a device key in each one dimensional array of the device key matrix, and (ii) a device ID indicates a path in a plurality of trees that are formed of all possible combinations of device keys in the device key matrix, as now specifically required in independent claims 1 and 9.

Thereby, amended independent claims 1 and 9, and the claims dependent therefrom, are believed to clearly distinguished over Shimbo.

Moreover, no teachings in Bleichenbacher were cited with respect to the above-noted features, nor are any teachings in Bleichenbacher believed to cure the above-noted deficiencies in Shimbo.

In view of these foregoing comments, applicants respectfully submit the claims as currently written distinguish over the applied art.

As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Surinder Sachar
Registration No. 34,423

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 03/06)

I:\ATTY\SNS\21'S\219406\219406US-AM.DOC